REMARKS

Claims 1-67 are pending in the application. Claims 1-67 are rejected. Claims 1, 3, 8, 13-14, 16, 27-28, 32-33, 35, 40, 45-46, 48, 59-60 and 66-67 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 5,457,747 to Drexler et al. in view of "Fingerprint Technology Makes for Best ID System" ("Rechtin"). Claims 1-2, 4-7, 9-12, 15, 17-26, 29-32, 34, 36-39, 41-44, 49-58 and 61-65 stand rejected under U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 5,457,747 to Drexler et al. in view of "Is it Time for Biometrics" ("Biometrics").

Reconsideration is requested. The rejections are traversed. No new matter is added. Claims 1, 4, 7, 18-19, 23-24, 26, 29, 32, 36, 39, 50-51, 55-56, 58, and 64-65 are amended. Claims 17, 29, 49, and 57 are canceled. Claims 68-69 are added. Claims 1-16, 18-28, 30-48, 60-56, and 58-69 remain in the case for consideration.

Claims 1 and 32 are amended to incorporate the features of previous dependent claims 17 and 49, which are hereby canceled.

This patent application is a continuation-in-part of U.S. Patent Application Serial No. 09/398,914 filed September 16, 1999, now pending, which is a continuation-in-part of U.S. Patent Application Serial No. 09/244,784 filed February 5, 1999, now U.S. Patent No. 6,012,039. The Applicant suggests the Examiner review these cases, to determine whether a double-patenting rejection might be appropriate.

REJECTIONS UNDER 35 U.S.C. § 103(a)

In rejecting former claims 17 and 49, the Examiner argues that Drexler teaches a rule-module formation step in column 7, lines 18-50 and column 8, lines 22-27, a rule-module invocation step in column 7, lines 39-43, and column 8, lines 22-27, and an electronic communication execution step upon invocation of a user-customized rule-module at column 7, lines 39-43, and column 8, lines 22-27. The Applicant respectfully disagrees.

Drexler does not teach or suggest a rule-module as claimed

A rule-module is a way to associate an execution command with a particular pattern data. Once a user has been successfully identified, rule-modules for that user can be invoked. If the appropriate pattern data is provided, the associated execution command can be executed. An example of how this can work is for age verification, for example to purchase alcohol. The data processing center (DPC) can identify the user via biometric data. The DPC can then access the user's age (demographic information). A rule-module states that a user's demographic information must show that the user is over a particular age (e.g., 21) to purchase alcohol at a particular location; if the user is not old enough, then the transaction is blocked (by an execution command). When this rule-module is invoked, if the user is not old enough to purchase alcohol given the user's location, and the transaction is a purchase that includes alcohol, the execution command of the rule-module can be used to block the transaction from being completed.

The above example is one for a rule-module that might be defined for all users, and might not be specific to an individual user. But it should be apparent how rule-modules could be defined that are specific to the user. For example, a user might set up a rule that says that any transaction that exceeds some threshold value (say $500) could cause an e-mail to be sent to the user's e-mail account, to warn the user of the potential for identity theft. Such a rule-module is an example of a rule-module that a user could define for himself, rather than one established to guarantee compliance with local laws (and so applicable to all users).

The Applicant sees nothing in Drexler that comes close to the concept of a rule-module. A description of how Drexler operates might be helpful. When a user registers with the system of Drexler, the biometric information is first sent to the library (*see* Drexler, column 7, lines 35-37). If the biometric information matches biometric information under "a different name, social security number or other common identification" (*see* Drexler, column 7, lines 40-42), the authorization for benefits is denied, and the system suggests the user be apprehended (*see* Drexler, column 7, lines 39-44). (Nowhere does Drexler explain how the biometric information can be compared with all the information in the library in real-time, which suggests that this comparison is done in an off-line manner, taking as much time as necessary. Put another way, this comparison is not done "while the user waits".) Otherwise, the system stores the biometric information in the library, along with the name and other identification data (*see* Drexler, column 7, lines 44-48). The biometric information is then "recorded indelibly on a card" (*see* Drexler, column 7, lines 51-52). The system also accommodates situations such as lost or stolen cards (*see* Drexler, column 7, lines 52-63).

When the user attempts to verify his identity (note that Drexler describes the user as using a "verification terminal" (*see* Drexler, column 7, line 64)), the biometric information is acquired from the user, and also read from the card (*see* Drexler, column 7, lines 64-66). The biometric information acquired from the user and read from the card are compared (*see* Drexler, column 8, lines 1-2). If the comparison does not indicate a successful match (even after repeating the data acquisition and comparison steps), then authorization is denied, and the system recommends the user be apprehended (*see* Drexler, column 8, lines 3-7).

If the comparison indicates a match (that is, the user's identity is verified at the verification terminal), and if the verification terminal is connected to the library, then additional steps might be performed. First, the biometric information is sent to the library (*see* Drexler, column 8, lines 7-13). The library checks to see if the biometric information is corresponds to "a different name or other common identification" (*see* Drexler, column 8, lines 15-16), then authorization is denied, and the system recommends the user be apprehended (*see* Drexler, column 8, lines 14-17). (Again, Drexler does not explain how such a check can be made in real-time, to avoid the user having to unduly wait for verification of his identity.) The library also checks to see if a replacement card had been issued, but the card used at the verification terminal was not the replacement card, then authorization is denied and the system recommends the user be apprehended (*see* Drexler, column 8, lines 17-22). Otherwise, if the library confirms the verification of the user's identity (that is, the library stores the biometric information corresponding to the same name and other common identification information), then the library signals the verification terminal authorizing the transaction (*see* Drexler, column 8, lines 22-27).

From the above description, Drexler does not describe a rule-module as claimed. First, the rule-module is claimed as "a user-customized rule-module" (*see, e.g.*, claim 1). Nothing in the library of Drexler is "user-customized": the decision whether to permit the user to enroll at the library, and the decision at the library that the user has not registered multiple times or is holding an outdated card, is all defined by the system developer. The user has no input into controlling how the library does what it does.

In rejecting former claims 25 and 57, the Examiner argued that Drexler teaches user-customized execution commands in that if there is no match for the biometric in the library, then the information is stored in the library. The Applicant respectfully disagrees that this concept anticipates the claimed feature. The "command" the Examiner is relying upon is not described anywhere as "user-customized" in Drexler, and this "command" is, in fact, a principal of operation of the library; it cannot be "customized" by any user. Accordingly, Drexler does not teach a user-customized execution command.

Second, according to Drexler, "[m]ost verification terminals would not be connected through telecommunications to the library" (*see* Drexler, column 8, lines 7-9). As such, in most situations, the library is not involved in verifying the user's identity, and therefore is not involved in authorizing or denying the transaction. Put another way, unless the verification terminal happens to be capable of communicating with the library, the verification terminal determines whether the user's identity is verified or not by itself, without involving the library. Thus, if, as the Examiner suggests, the library is responsible for storing and invoking rule-modules, in most situations a rule-module cannot be used at all.

Third, even when the library is involved in verifying the user's identity, the only concepts Drexler describes that even approach a rule-module are the denial of the user's request for benefits, along with the suggestion to apprehend the user. But these actions occur only if "the information matches biometric information at the library corresponding to a different name or other common identification . . . [or] if the information matches that at the library but the library indicates that a replacement card has been issued and the information on the card lacks the additional information indicating that it is a replacement card" (*see* Drexler, column 8, lines 14-16 and 17-21). In other words, these actions, the closest analog in Drexler to the concept of an execution module, are invoked only if the user is determined to have a fraudulent identity. But if the user has a fraudulent identity, then the rule-module cannot be invoked "upon a successful identification of the user", as claimed (*see, e.g.*, claim 1).

The Examiner might argue that Drexler teaches a rule module in the concept of the library "authorizing limited benefits" (*see* Drexler, column 8, line 26), which occurs after the library has verified the user's identity (as already verified at the verification terminal). The Applicant respectfully suggests that when Drexler describes "authorizing limited benefits", Drexler is doing nothing more than authorizing a transaction, which is analogous to the electronic communication step of claim 1, or the electronic communication authorization platform of claim 32. In the claimed invention, the authorization of a communication is separate from the execution of an execution module in a rule-module. The better analog for the "authorize[ed] limited benefits" of Drexler is the authorization of the electronic communication, which means that Drexler does not teach an execution command as claimed.

In addition, Drexler describes the library as "a library of biometric information" (*see* Drexler, column 6, lines 18-19). Nowhere does Drexler describe the library as storing more than the biometric information. While Drexler might describe the library as being able to deny authorization of a request for benefits, this is a far cry from describing the library as storing rule-modules that include pattern data and execution commands. And, as argued above, the claimed rule-module is invoked upon successful identification of the user: Drexler does not teach that anything is invoked upon successful identification of the user, let alone a rule-module that includes pattern data and an execution command. In fact, Drexler does not describe anything that happens after successful identification; any such actions are beyond the scope of Drexler.

Finally, where the Applicant uses different terms in the same claim, the Applicant intends that there are two separate features claimed, rather than a single feature described using two different names. (If the Applicant used the different terms to describe the same claim feature, the Examiner would be within her rights to reject the claims as indefinite under 35 U.S.C. § 112, ¶ 2.) As the Applicant has recited both an "electronic communication" and an "execution command" in the claims, these terms describe different features, and cannot be taught by the same feature of a prior art reference. Thus, even if the Examiner's argument that Drexler's "authorizing limited benefits" is analogous to the execution command in the rule-module, the consequence of this argument would mean that Drexler does not teach or suggest an analog for the authorization of the electronic communication recited in the claims.

"Biometrics" does not support the rejection

"Biometrics" is only one paragraph long. The Examiner argues that "Biometrics" discloses biometrically-authorizing electronic communications without the user having to present smartcards or magnetic swipe cards (*see, e.g.*, Office Action dated June 13, 2008, page 4). The Applicant respectfully disagrees.

First, "Biometrics" is not a patent. Therefore, there is no presumption of validity under 35 U.S.C. § 282. Further, under M.P.E.P. 2121, the prior art must be enabling. M.P.E.P. 2121 states that "[w]hen the reference relied on expressly anticipates or makes obvious all of the elements of the claimed invention, the reference is presumed to be operable". But it is important to remember that this presumption applies **only if** the reference "expressly anticipates or makes obvious **all** of the elements of the claimed invention" (*see* M.P.E.P. § 2121; emphasis added). The Examiner cites to "Biometrics" only for the concept of biometrically-authorizing an electronic communication without using smartcards or magnetic swipe cards. The Applicant suggests that "Biometrics" suggests no other feature recited in the claims; certainly, "Biometrics" does not teach or suggest **all** of the "elements of the claimed invention". Therefore, even the presumption that "Biometrics" is enabling is not available to the Examiner.

Second, the Applicant suggests that, in fact, "Biometrics" is not an enabling disclosure. Even if "Biometrics" could be read as suggesting that a biometric transaction could be performed without smartcards or magnetic swipe cards, the Applicant does not see how such a feat could be accomplished by combining "Biometrics" with Drexler. Certainly Drexler, which even the Board of Patent Appeals and Interferences acknowledged teaches a token-based system (*see* Decision on Appeal 2007-2591, page 9), does not enable a person of ordinary skill in the art to implement a tokenless biometric authorization system. But if "Biometrics" does not teach how to implement the specific teaching for which the Examiner relies upon "Biometrics", then "Biometrics" is not an enabling reference. And as the M.P.E.P. states that "[a] prior art reference provides an enabling disclosure . . . if the reference describes the claimed invention in sufficient detail to enable a person of ordinary skill in the art to carry out the claimed invention" (*see* M.P.E.P. § 2121), by implication a reference does not provide an enabling disclosure if there is insufficient detail "to enable a person of ordinary skill in the art to carry out the claimed invention". "Biometrics" provides **no** detail at all, and therefore cannot be enabling.

The Applicant acknowledges that in an obviousness rejection under 35 U.S.C. § 103(a), the reference does not need to be enabling in its entirety (*see* M.P.E.P. § 2121.01). But the M.P.E.P still requires that the reference teach something: the reference is prior art as to what it actually teaches. All that "Biometrics" says is that one can do biometric identification, without any further detail. So the entirety of what "Biometrics" teaches is that one can do biometric identification in some (undescribed) manner.

The Applicant also disagrees with the Examiner that "Biometrics" teaches a tokenless biometric system. "Biometrics" states that "Fingerprint identification is currently being test marketed although it requires the use of smart cards and some individuals' prints cannot be easily read. Also, the retina patterns of a cardholder's eye can be scanned. Other methods being considered include hand geometry, hand vein checking, keystroke dynamics, voice identification, and signature verification". "Biometrics" acknowledges that when using fingerprints for identification, smartcards are required. The Applicant believes that "Biometrics" only suggests retina patterns, hand geometric, hand vein checking, keystroke dynamics, voice identification, and signature verification can be substituted for fingerprints, which would mean that these other biometrics would also require the use of a smartcard. If "Biometrics" had intended to suggest that these other biometrics could be used without a smartcard, "Biometrics" would have mentioned them first (as they would clearly be superior to the token-based identification system using fingerprints), or would have stated that these biometrics could be used without needing a smartcard (to distinguish them from fingerprints). The Applicant suggests that reading "Biometrics" as teaching the use of these non-fingerprint biometrics as operating tokenlessly is to interpret "Biometrics" far more broadly than described.

Another point against reading "Biometrics" as teaching biometric identification without a token is that "Biometrics" does not explain why fingerprint identification "requires the use of smart cards". The reasonable interpretation as to why "Biometrics" "requires" a smart card for fingerprint identification is that it is difficult to match a single fingerprint against a large database of fingerprints. But that is precisely the same reason why Drexler uses a card: to reduce the problem to that of verifying the user's identity with a biometric. Further, replacing "fingerprint" with any of the other biometrics described in "Biometrics" does not simplify the problem of comparing one biometric against a large database of biometrics: comparison of these other biometrics is just as complicated as fingerprint comparison (or else these other biometric comparison systems would have replaced fingerprint verification a long time ago). Thus, using any of these other biometrics would still require the use of a smartcard in "Biometrics".

Third, the Applicant does not believe one can combine Drexler with "Biometrics". As described above, Drexler stores the biometric on a card, and verifies the user's identity by reading the biometric information from this card. The information read from the card is then compared with biometric information retrieved from the user. If the comparison fails, then the system blocks the transaction (*see* Drexler, column 7, line 64 through column 8, line 7). But if the comparison succeeds, then the library is queried to double-check the verification terminal. (The Applicant is following the Examiner's argument in the rejection of the claims, as the Examiner has relied on the operation of the library as teaching features of the claimed invention.) If the library confirms the verification of the user's identity, then the library signals the verification terminal, authorizing limited benefits, "which are recorded on the card on the temporary storage medium" (*see* Drexler, column 8, lines 26-27). By storing the authorized limited benefits on the temporary storage medium of the card, Drexler makes it possible for "a plurality of existing benefit dispensers at other locations, such as automated teller machines, [to read the authorized benefits,] which can then dispense benefits authorized by the data" (*see* Drexler, Abstract, lines 15-18). In other words, the card in Drexler is not used just to store the biometrics on a token; it is also used to store other information used by Drexler, which can then be read by other terminals that can dispense the benefits. The card in Drexler also stores information about which card it is: is it the original card issued to the user, or is it a replacement card?

In other words, the card in Drexler stores information that is used after the user's successful verification. The Examiner has not explained how Drexler could be modified to eliminate the token, in the combination with "Biometrics", as the card is used for other purposes than just to store biometric information. Put another way, eliminating the card from Drexler requires changing its operation to address the issue of replacement cards and how other devices can rely on the user's verification at the verification terminal. Accordingly, the Applicant believes that the combination of Drexler and "Biometrics" would render Drexler unsatisfactory for its intended purpose (M.P.E.P. § 2143.01). The Applicant also believes that the result of combining Drexler and "Biometrics" would not be predictable, given that they (potentially) conflict on the necessity of a smartcard (*see* M.P.E.P. § 2143.01). (The Applicant also notes that these same arguments apply with respect to the combination of Drexler and Rechtin.)

The Examiner argues that "'the combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results'" (*see, e.g.*, Office Action dated June 13, 2008, pages 4 and 10). The Applicant respectfully disagrees. First, the Applicant believes that the Examiner has failed to make the necessary factual findings to support a rejection of obviousness. "When making an obviousness rejection, Office personnel must therefore ensure that the written record includes findings of fact concerning the state of the art and the teachings of the references applied. In certain circumstances, it may also be important to include explicit findings as to how a person of ordinary skill would have understood prior art teachings, or what a person of ordinary skill would have known or could have done. Factual findings made by Office personnel are the necessary underpinnings to establish obviousness" (*see* M.P.E.P. § 2141). The Examiner has made no factual findings whatsoever in this case with respect to the supposed teachings of "Biometrics": in particular, as to how a tokenless biometric system could be implemented.

Second, the Examiner has not explained what "known methods" could be used to combine Drexler and "Biometrics". Given that "Biometrics" says literally nothing about how a tokenless biometric system could be implemented, the Applicant does not believe there are any "known methods" as to how Drexler could be converted into a tokenless system. Even Rechtin, another non-patent reference, describes a scenario in which tokenless biometric systems could operate in an ideal world, but does not describe exactly how such systems would actually work. As such, the Applicant does not believe the Examiner has established a tokenless biometric system as a "familiar element", and therefore there are no "known methods" for combining such an unknown system with Drexler. Further, the Applicant does not believe the results of such a combination would "yield predictable results": if Drexler relies on the storage mediums on the card, both to perform a biometric comparison and to store the limited authorized benefits, it is completely unpredictable how Drexler would operate when the card is removed from the system.

The Applicant notes that the Supreme Court in KSR Int'l Co. v. Teleflex Inc., 127 S. Ct. 1727 (2007) described three cases that came after Graham v. John Deere Co., 383 U.S. 1, 148 U.S.P.Q. 459 (1966)), in which the combination of familiar elements according to known methods supported an obviousness rejection. In United States v. Adams, the alternation of a known structure by substituting one element for another known in the field was considered obvious. In Anderson's-Black Rock, Inc. v. Pavement Salvage Co., the two pre-existing elements in combination did nothing more than they would in separate, sequential operation. And in Sakraida v. AG Pro, Inc., arranging old elements, each performing the same function it had performed in the past, was obvious. But the facts of this case are different from each of these three cases. In contrast with *Adams*, the Applicant does not believe the Examiner has established that tokenless biometric systems were known before the filing date of the claimed invention; in any event, Drexler is a token-based system, and removing the token from Drexler is considerably more involved than just substituting one element for another in a known structure. In contrast with *Anderson's-Black Rock*, tokenless and token-based systems are very different, and combining the two does not achieve the same result as running the two sequentially (which, after all, in the proposed combination would result in the user being identified/verified twice). And in contrast with *Sakraida*, the combination of Drexler and "Biometrics" does not arrange old elements, each performing the same function: because the token has to be removed from Drexler in the combination of Drexler and "Biometrics", the operation of Drexler in the combination of Drexler and "Biometrics" is different from its separate operation. Accordingly, the combination of Drexler and "Biometrics" is not "the combination of familiar elements according to known methods", despite the Examiner's assertion to the contrary.

New claim 68 is similar to claim 1, except that it does not include the features relating to registration of the user's biometric sample. All of the arguments relating to claim 1 are also applicable to new claim 68.

As the combination of Drexler and "Biometrics" does not teach a user-customized rule-module that can be invoked upon successful identification of the user or a user-customized execution command, as "Biometrics" does not teach a tokenless biometric system, as "Biometrics" is not an enabling disclosure as to how to implement a tokenless biometric system, and as the combination of Drexler and "Biometrics" leaves unclear how the token could be eliminated from Drexler without substantially changing its operation, claims 1, 32, and 68 are patentable under 35 U.S.C. § 103(a) over Drexler in view of "Biometrics".

Accordingly, claims 1, 32, and 68 are allowable, as are dependent claims 2-16, 18-28, 30-31, 33-48, 60-56, 58-67, and 69.

In rejecting claims 18, 50, and 64-65, the Examiner argues that Drexler teaches pattern data at column 7, lines 18-50. The only descriptions the Applicant sees there, or anywhere else in Drexler, that appears to meet the description of pattern data are the use of names, social security numbers, or other identifications, and the biometric. Claims 18, 50, and 64-65 have been amended to remove reference to the pattern data including a biometric and a user unique identification code. (By a significant stretch of the imagination, a social security number might be considered a user unique identification code, as it is unique. But as people are actively discouraged, even by the federal government, from using their social security numbers as identifiers, and not everyone has a social security number, the Applicant does not believe that a social security number properly meets the definition of a "user unique identification code". Nevertheless, in the interest of furthering allowance of this application, the Applicant has removed "a user unique identification code" from the recitation of pattern data.) Accordingly, the Applicant believes that claims 18, 50, and 64-65 are patentable under 35 U.S.C. § 103(a) over Drexler in view of "Biometrics", and are therefore allowable.

In rejecting claims 19 and 51, the Examiner argues that Drexler teaches "execution commands including user-customized instructions for executing any of the following: accessing of stored electronic data, processing (initiation) of electronic data (apprehension measures), and presentation of electronic data" (*see* Office Action dated June 13, 2008, page 14). The Applicant respectfully disagrees. First, initiating apprehension measures does not meet the definition of processing of electronic data: apprehension of an individual is a physical act, and does not involve the processing of electronic data in any form. Second, even if initiating apprehension measures was analogous to processing of electronic data, such a command is not "user-customized", as recited in the claims. Such a command is defined by the system administrator, and not by the user who defined the rule-module. Further, "Biometrics" does not teach or suggest these features.

As the combination of Drexler and "Biometrics" does not teach or suggest user-customized instructions, claims 19 and 51 are patentable under 35 U.S.C. § 103(a) over Drexler in view of "Biometrics". Accordingly, claims 19 and 51 are allowable, as are dependent claims 20-22, 52-54, and 64-65.

In rejecting claim 2, the Examiner argues that Drexler teaches the electronic indicated storing a subset of all the registration biometric samples (*see* Office Action dated June 13, 2008, pages 4-5). The only analog to the "electronic identicator" in Drexler is the library. But nowhere does Drexler teach or suggest that the library could be subdivided. "Biometrics" also fails to teach or suggest this feature. Accordingly, claim 2 is patentable under 35 U.S.C. § 103(a) over Drexler in view of "Biometrics", and is allowable

In rejecting claims 4 and 36, the Examiner argues that the verification terminal performs the first comparison step, and that the library performs the second comparison step (*see* Office Action dated June 13, 2008, page 5). The Applicant acknowledges that Drexler discloses the possibility of both the verification terminal and the library performing a comparison. But the Applicant respectfully suggests the Examiner has not considered the claim in its entirety. First, as argued above, according to Drexler most verification terminals are not connected to the library. This means that the verification terminal cannot refer the biometric to the library for a second comparison at all.

Second, and more importantly, the verification terminal in Drexler transmits the biometric information to the library **only if** "the information of the card and the possessor of the card match" (*see* Drexler, column 8, lines 11-12). As a consequence, if the verification terminal decides that the comparison failed, there is no referral of the biometric information to the library. This makes complete sense: if the system is certain that the possessor of the card has no right to use the card, then there is no need to make any further comparisons at the library. The library is involved in verifying the user's identity **only if** the verification terminal confirms the user's identity. And even then, the library in Drexler is only double-checking that the user has not registered with the system multiple times, or is using an outdated card. Put another way, the library is trusting that the original determination by the verification terminal that the user matched the biometric information on the card was correct.

Given that claims 4 and 36 recite "if the subset electronic identicator returns a failed identification result, the bid biometric sample is electronically transmitted via a public communications network to a master electronic identicator" (*see, e.g.*, claim 4), it is a necessary precondition to the second comparison that the first comparison failed. As discussed above, in Drexler, if the first comparison fails, there is no second comparison at the library. Accordingly, Drexler does not teach the features of the claimed invention. Further, "Biometrics" also fails to teach or suggest this feature.

As the combination of Drexler and "Biometrics" does not teach or suggest a second comparison if the first comparison fails, claims 4 and 36 are patentable under 35 U.S.C. § 103(a) over Drexler in view of "Biometrics". Accordingly, claims 4 and 36 are allowable, as is dependent claim 69.

In rejecting claims 5 and 37, the Examiner argues that a person can be an "enterprise". The Applicant respectfully disagrees. According to the specification, "[a]n enterprise is any legally formed entity, such as a corporation, a non-profit organization, and the like. An individual user is any person who electronically communicates with an enterprise, often as a customer or supplier of the products and services provided by the enterprise" (*see* specification, page 27, lines 26-29). From this description, it is clear that a "person" is distinguishable from an "enterprise".

During examination of a patent application, "the pending claims must be 'given their broadest reasonable interpretation consistent with the specification'" (*see* M.P.E.P. 2111). Given that the specification defined the term "enterprise" to include "legally formed entit[ies]", a person, who is not a legally formed entity, is not an enterprise.

The Examiner might argue that it is improper to import claim limitations from the specification (*see* M.P.E.P. § 2111.01). The Applicant respectfully points out that the terms are still entitled to their plain meaning, and that a person of ordinary skill in the art would understand that a person is not an enterprise. The closest that a "person" comes to being an enterprise is when the person is operating a sole proprietorship. But even in that situation, the business operated by the person is a legally formed entity, and is distinguishable from the person individually. A person of ordinary skill in the art would understand this distinction, and would understand that a "person" is not an entity.

As per the above discussion, Drexler does not teach an "enterprise" that can be involved in enterprise registration, enterprise bid identity transmission, or enterprise identification. "Biometrics" also fails to teach or suggest this feature. Therefore, claims 5 and 37 are patentable under 35 U.S.C. § 103(a) over Drexler in view of "Biometrics". Accordingly, claims 5 and 37 are allowable, as are dependent claims 6-7, 9, 15, 38-39, 41, 43, and 47.

In rejecting claims 9 and 41, the Examiner argues that Drexler teaches a corporation, such as a bank (*see* Office Action dated June 13, 2008, page 11). While Drexler does mention "welfare or social security office, or bank" (*see* Drexler, column 4, lines 33-34), the

Applicant respectfully disagrees that Drexler teaches the features of the claims. In particular, the "enterprise" recited in claims 9 and 41 is to be identified (as recited in parent claims 5 and 37). Nowhere does Drexler teach or suggest that the "bank" can be identified. "Biometrics" also fails to teach this feature. Accordingly, claims 9 and 41 are patentable under 35 U.S.C. § 103(a) over Drexler in view of "Biometrics", and are therefore allowable.

In rejecting claims 20 and 52, the Examiner argues that a "card" can be "unlocked" via authorization (*see* Office Action dated June 13, 2008, page 14). The Applicant respectfully disagrees.

First, according to the Examiner's proposed combination of Drexler and "Biometrics", the card of Drexler (that is, the token) is to be eliminated, so that the combination is tokenless (*see, e.g.*, Office Action dated June 13, 2008, page 4). If the card of Drexler is to be eliminated, then it can hardly be "authorized".

Second, the Applicant respectfully suggests that Drexler teaches authorizing "benefits" (*see, e.g.*, Drexler, column 8, line 26), not a card. These benefits can be "dispensed" by "dispensers" (*see, e.g.*, Drexler, Abstract, lines 16-17). Accordingly, there is no "secured physical device" in Drexler that can be "unlocked".

Third, even if the card of Drexler met the recited claim feature of a "secured physical device", that does not mean that the card can be "unlocked". The specification provides examples of how a secured physical device could be unlocked. If a user desires access to an Internet-connected medicine cabinet or to a gated mechanism, the user can provide a biometric. Once the user is identified by the system, the system can automatically unlock the medicine cabinet or the gated mechanism using an electromagnetic locking/unlocking mechanism (*see, e.g.*, specification, page 49, lines 14-19). In other words, claims 20 and 52 are directed to gaining physical access to some physical object protected by a locking mechanism. Authorizing a card does not meet this physical structure.

As argued above, Drexler does not teach or suggest unlocking a secured physical device. "Biometrics" also fails to teach this feature. Accordingly, claims 20 and 52 are patentable under 35 U.S.C. § 103(a) over Drexler in view of "Biometrics", and are therefore allowable.

In rejecting claims 26, 29, 58, and 63, the Examiner argues that the claimed feature of subset rule-module storage is taught in Drexler by the concept of "verification terminals or first writing devices" (*see* Office Action dated June 13, 2008, pages 16-17). The Applicant respectfully disagrees. Nowhere does Drexler describe the verification terminals or the first writing devices as storing anything, let alone rule-modules that are user-customized. The verification terminals are used to verify the user's identity, by comparing the user's biometric information with the information stored on the card; this comparison either succeeds or fails. But either way, the verification terminals do not store any user-customized rule-modules that include pattern data and execution commands.

As for the first writing modules, Drexler uses these to capture the user's biometric data and to generate the card. Again, nowhere does Drexler describe the first writing modules as storing any rule-modules, let alone user-customized rule-modules.

As argued above, Drexler does not teach the verification terminals or first writing devices as storing a subset of rule-modules. "Biometrics" also fails to teach this feature. Accordingly, claims 26, 29, 58, and 63 are patentable under 35 U.S.C. § 103(a) over Drexler in view of "Biometrics", and are therefore allowable, as are dependent claim 30-31 and 62.

For the foregoing reasons, reconsideration and allowance of claims 1-69 of the application as amended is requested. The Examiner is encouraged to telephone the undersigned at (503) 222-3613 if it appears that an interview would be helpful in advancing the case.

Respectfully submitted,

MARGER JOHNSON & McCOLLOM, P.C.

Ariel S. Rogson
Reg. No. 43,054

MARGER JOHNSON & McCOLLOM, P.C.
210 SW Morrison Street, Suite 400
Portland, OR 97204
503-222-3613

Customer No. 60460